PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference F-135-PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. **PCT/KR00/00640**	International filing date *(day/month/year)* 17 JUNE 2000 (17.06.2000)	Priority date *(day/month/year)* 17 JUNE 1999 (17.06.1999)

International Patent Classification (IPC) or national classification and IPC

IPC7 H04B 1/00

Applicant

KIM, Donggyun et al

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demamd	Date of completion of this report
17 JANUARY 2001 (17.01.2001)	28 JUNE 2001 (28.06.2001)
Name and mailing address of the IPEA/KR Korean Intellectual Property Office Government Complex-Daejeon, Dunsan-dong, Seo-gu, Daejeon Metropolitan City 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer JEONG, Hyun Su Telephone No. 82-42-481-5949

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

rnational aplication No.
PCT/KR00/00640

I. Basis of the report

1. With regard to the elements of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-14 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the claims:
pages 15-19 , as originally filed
pages NONE , as amended (together with any statment) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the drawings:
pages 1-2 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language English which is

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[X] the language of publication of the international application(under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide** and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained inthe international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disc losure in the international applicationas as filed has been furinshed.

[ ] The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. [ ] The amendments have resulted in the cancellation of:

[ ] the description, pages

[ ] the claims, Nos.

[ ] the drawings, sheet.

5. [ ] This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box(Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed." and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item I and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION

International aplication No.
PCT/KR00/00640

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-6	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-6	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-6	YES
	Claims	NONE	NO

2. Citations and explanations (Rule 70.7)

Reference is made to the following documents:
D1 : US 5872846
D2 : KR 98-77685
D3 : KR 98-35958

NOVELTY(N) Claims 1 to 6

The subject-matter according to claims 1 to 6 is novel pursuant to Art. 33(2) PCT.

D1 is considered to represent the most relevant state of the art.
It discloses a system and method for providing security in DATA communication systems where multiple users are coupled to a common receiving system.
The subject matter of present claims 1 and 6 differs therefrom in that it provides a public key transmission system of an improved knapsack type for securing higher safety by increasing transmission efficiency by easily producing an public key and hardly extracting a private key from the public key.

INVENTIVE STEP(IS) Claims 1 to 6

D1, D2 and D3 don't have particular relevance to the present invention.
D2 discloses a method producing a public key and a public key cryptosystem using said method, and D3 discloses the method using random function in producing public key.
The subject-matter of claim 1 is considered as inventive, since it refers to a improved process which is not known or even suggested in the art and in particular in D1, D2 and D3.
As a consequence, the subject-matter of the dependent claims 2 to 6 is also inventive.

INDUSTRIAL APPLICABILITY(IA) Claims 1 to 6

All claims are considered to be industrially applicable

COPY FOR IB

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Artcle 36 and Rule 70)

Applicant's or agent's file reference F-135-PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. **PCT/KR00/00640**	International filing date *(day/month/year)* 17 JUNE 2000 (17.06.2000)	Priority date *(day/month/year)* 17 JUNE 1999 (17.06.1999)

International Patent Classification (IPC) or national classification and IPC

IPC7 H04B 1/00

Applicant

KIM, Donggyun et al

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demamd	Date of completion of this report
17 JANUARY 2001 (17.01.2001)	28 JUNE 2001 (28.06.2001)

Name and mailing address of the IPEA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, Dunsan-dong, Seo-gu, Daejeon Metropolitan City 302-701, Republic of Korea	JEONG, Hyun Su
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5949

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

[redacted]ational aplication No.
PCT/KR00/00640

I. Basis of the report

1. With regard to the elements of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-14 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the claims:
pages 15-19 , as originally filed
pages NONE , as amended (together with any statment) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the drawings:
pages 1-2 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language English which is

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[X] the language of publication of the international application(under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide** and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained inthe international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disc losure in the international applicationas as filed has been furinshed.

[ ] The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. [ ] The amendments have resulted in the cancellation of:

[ ] the description, pages

[ ] the claims, Nos.

[ ] the drawings, sheet

5. [ ] This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box(Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed." and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item I and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION

national aplication No.
PCT/KR00/00640

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-6	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-6	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-6	YES
	Claims	NONE	NO

2. Citations and explanations (Rule 70.7)

Reference is made to the following documents:
D1 : US 5872846
D2 : KR 98-77685
D3 : KR 98-35958

NOVELTY(N) Claims 1 to 6

The subject-matter according to claims 1 to 6 is novel pursuant to Art. 33(2) PCT.

D1 is considered to represent the most relevant state of the art.
It discloses a system and method for providing security in DATA communication systems where multiple users are coupled to a common receiving system.
The subject matter of present claims 1 and 6 differs therefrom in that it provides a public key transmission system of an improved knapsack type for securing higher safety by increasing transmission efficiency by easily producing an public key and hardly extracting a private key from the public key.

INVENTIVE STEP(IS) Claims 1 to 6

D1, D2 and D3 don't have particular relevance to the present invention.
D2 discloses a method producing a public key and a public key cryptosystem using said method, and D3 discloses the method using random function in producing public key.
The subject-matter of claim 1 is considered as inventive, since it refers to a improved process which is not known or even suggested in the art and in particular in D1, D2 and D3.
As a consequence, the subject-matter of the dependent claims 2 to 6 is also inventive.

INDUSTRIAL APPLICABILITY(IA) Claims 1 to 6

All claims are considered to be industrially applicable

02

RECORD COPY

10/018944

PCT REQUEST

f-135-pct

Original (for **SUBMISSION**) - printed on 17.06.2000 11:45:19 AM

0 0-1	**For receiving Office use only** International Application No.	PCT/KR 00/00640
0-2	International Filing Date	17 June 2000 (17.06.00)
0-3	Name of receiving Office and "PCT International Application"	Korean Industrial Property Office P C T International Application
0-4 0-4-1	**Form - PCT/RO/101 PCT Request** Prepared using	PCT-EASY Version 2.90 (updated 10.05.2000)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Korean Industrial Property Office (RO/KR)
0-7	**Applicant's or agent's file reference**	f-135-pct
I	**Title of invention**	METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY
II II-1 II-2 II-4 II-5 II-6 II-7 II-8 II-9 II-10	**Applicant** This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence Telephone No. Facsimile No. e-mail	 applicant and inventor all designated States KIM, Donggyun KOREA University, anam-dong 5-1, seongbuk-gu 136-701 Seoul Republic of Korea KR KR 82-2-3290-3080 82-2-926-1110 dkim@semi.korea.ac.kr
III-1 III-1-1 III-1-2 III-1-3 III-1-4 III-1-5 III-1-6 III-1-7	**Applicant and/or inventor** This person is: Applicant for Inventor for Name (LAST, First) Address: State of nationality State of residence	 applicant and inventor US only US BAE, Jaegug dongsam-1dong, youngdo-gu 606-081 Pusan Republic of Korea KR KR

PCT REQUEST

f-135-pct

Original (for **SUBMISSION**) - printed on 17.06.2000 11:45:19 AM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	PARK, Hae-sun
IV-1-2	Address:	yoksam-dong 824-19, gangnam-gu 135-080 Seoul Republic of Korea
IV-1-3	Telephone No.	82-2-554-7561
IV-1-4	Facsimile No.	82-2-557-9121
IV-1-5	e-mail	koreana@koreanap.co.kr
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	CHO, Young-won
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

WITHDRAWN BY APPLICANT

PCT REQUEST

f-135-pct

Original (for **SUBMISSION**) - printed on 17.06.2000 11:45:19 AM

V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	17 June 1999 (17.06.1999)	
VI-1-2	Number	99-22638	
VI-1-3	Country	KR	
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1	
VII-1	**International Searching Authority Chosen**	Korean Industrial Property Office (KIPO) (ISA/KR)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	4	-
VIII-2	Description	16	-
VIII-3	Claims	8	-
VIII-4	Abstract	1	abstract.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	31	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-18	**Figure of the drawings which should accompany the abstract**		
VIII-19	**Language of filing of the international application**	Korean	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name (LAST, First)	PARK, Hae-sun	
IX-2	**Signature of applicant or agent**		
IX-2-1	Name (LAST, First)	CHO, Young-won	

PCT REQUEST

f-135-pct

Original (for **SUBMISSION**) - printed on 17.06.2000 11:45:19 AM

FOR RECEIVING OFFICE USE ONLY

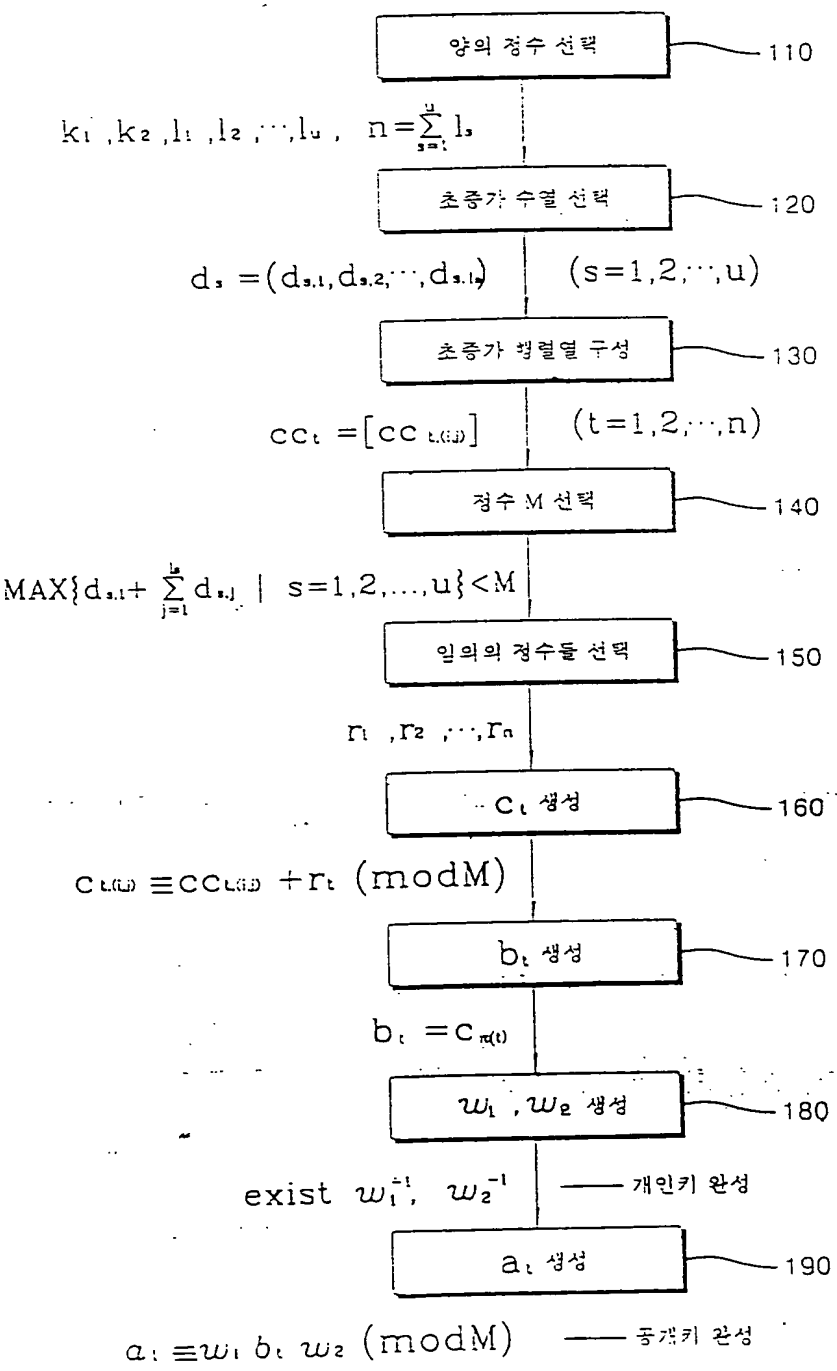
10-1	Date of actual receipt of the purported international application	17 June 2000 (17.06.00)
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/KR
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

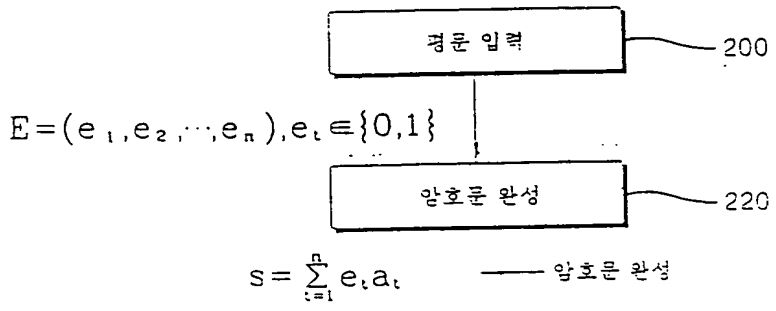
11-1	Date of receipt of the record copy by the International Bureau	17 JULY 2000 (17.07.00)

[도면]

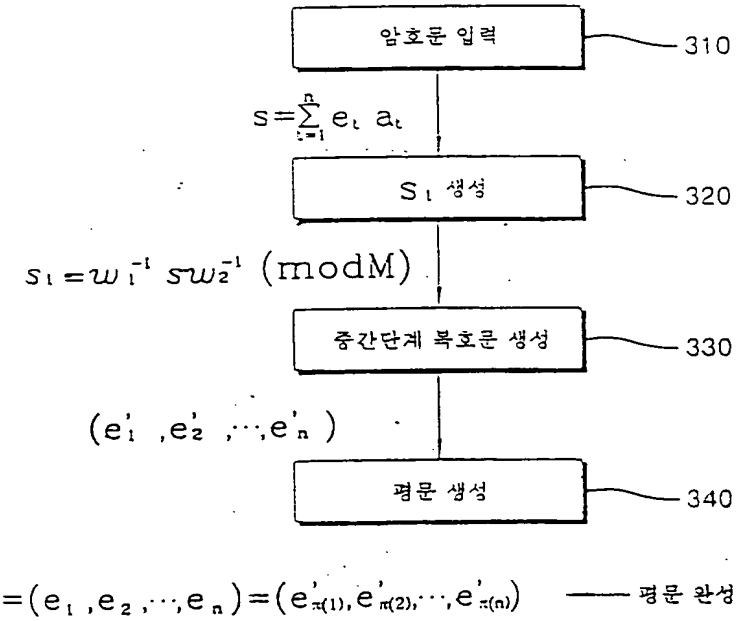
[도 1]


양의 정수 선택
110
$k_1, k_2, l_1, l_2, \cdots, l_u, \quad n=\sum_{s=1}^{u} l_s$
초증가 수열 선택
120
$d_s=(d_{s,1}, d_{s,2}, \cdots, d_{s,l_s}) \quad (s=1,2,\cdots,u)$
초증가 행렬열 구성
130
$cc_t=[cc_{t,(j)}] \quad (t=1,2,\cdots,n)$
정수 M 선택
140
$MAX\{d_{s,1}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u\}<M$
임의의 정수들 선택
150
$r_1, r_2, \cdots, r_n$
c_t 생성
160
$c_{t,(j)} \equiv cc_{t,(j)} + r_t \pmod{M}$
b_t 생성
170
$b_t = c_{\pi(t)}$
w_1, w_2 생성
180
exist $w_1^{-1}, \quad w_2^{-1}$
개인키 완성
a_t 생성
190
$a_t \equiv w_1 b_t w_2 \pmod{M}$
공개키 완성

[도 2]


평문 입력
200
$E=(e_1,e_2,\cdots,e_n), e_t \in \{0,1\}$
암호문 완성
220
$s=\sum_{t=1}^{n} e_t a_t$
암호문 완성

[도 3]


암호문 입력
310
$s=\sum_{t=1}^{n} e_t a_t$
s_t 생성
320
$s_t = w_1^{-1} s w_2^{-1} \pmod{M}$
중간단계 복호문 생성
330
$(e'_1, e'_2, \cdots, e'_n)$
평문 생성
340
$E=(e_1,e_2,\cdots,e_n)=(e'_{\pi(1)}, e'_{\pi(2)}, \cdots, e'_{\pi(n)})$
평문 완성

【명세서】

【발명의 명칭】

이진 정보 보호 전송방법{METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY}

【기술분야】

본 발명은 전자 전송매체를 통하여 이진정보를 전송하는 방법에 관한 것으로서, 특히 이진정보를 초증가 행렬렬을 이용하여 암호화하여 전송하고, 복호화하는 방법에 관한 것이다.

【배경기술】

근래에 전자 전송 매체를 통하여 정보를 전송하는 경우, 특히 컴퓨터간의 데이터 전송에 있어서 보안상의 문제가 점점 증가하고 있다. 실제로 전송로로부터 전송되는 데이터를 도청하기는 비교적 손쉬운 일이며, 이것은 중요한 정보가 제 3 자의 손으로 넘어갈 수 있다는 것을 의미한다. 이와 같은 위험을 방지하기 위해서 정보 전송시 제 3 자가 용이하게 판독하지 못하도록 정보를 암호화한 후 전송할 필요가 있다.

이를 위하여 다양한 형태의 암호화 방식이 제안되고 있다. 암호화 방식은 크게 대칭키에 의한 방식과 공개키에 의한 방식으로 나뉜다. 대칭키 방식은 암호화키와 동일한 복호화키를 사용하는 방식이고, 공개키에 의한 암호화 방식은 암호화키와 다른 복호화키를 사용하는 방식이다. 대칭키에 의한 암호화 방식은 일 대 일 데이터 전송에는 유용하지만 다 대 일 데이타 전송에는 각각이 서로 다른 암호화키를 사용해야 하므로 번잡한 문제가 따른다. 반면에, 공개키 방식은 일반에

게 공개된 공개키 와 수신자가 보유하는 개인키 한 쌍만 있으면 되므로 다 대 일 데이터 전송에 유용하다. 즉, 누구나 공개키로 전송하고자 하는 정보를 암호화하면 수신자는 자신이 갖고 있는 비밀키 즉 개인키로 이를 복호화할 수 있다.

이러한 공개키 암호화 방식은 2 가지 중요한 요소를 갖고 있다. 전송의 안전성과 전송의 효율성이 그것인데, 전송의 안전성은 수신자 아닌 제 3 자가 공개키로부터 개인키를 추출하는 것이 얼마나 곤란한가 여부에 따라 결정되며, 전송의 효율성은 공개키를 얼마나 용이하게 생성할 수 있는가 여부에 따라 결정된다.

공개키 전송시스템은 1976년 Diffie 와 Hellman 이 처음 소개한 이후로 수많은 연구가 진행되어 왔으며, 보다 안전한 시스템을 고안하려는 노력이 지속되어 왔다.

RSA는 1978년에 만들어진 공개키 전송시스템으로서 현재 세계시장에 90% 이상의 점유율을 갖고 있다. RSA 전송시스템은 정수의 소인수분해가 어렵다는 수학적 문제를 기본적인 암호화 방법으로 삼고 있다. 그러나 RSA 전송시스템은 암호화와 복호화에 상당한 시간이 소요된다는 단점을 가지고 있다.

즉, RSA 전송시스템은 암호키를 발생하는데 시간이 오래걸림으로써 정보의 전달이 지연되었다. 이것은 송신기의 정보의 전송비율을 낮추게 하거나 또는 전송비율을 조절하기 위하여 대용량의 버퍼 등을 구비하는 것을 필요하게 하였으며, 버퍼를 구비하는 경우는 수신국에서 정보를 수신할 준비가 되어 있지 않다는 신호를 발생할 때 정보가 손실되지 않도록 보장해 주는 조치가 수반되어야 한다.

한편, 이와 같은 RSA 전송시스템의 문제를 극복할 수 있는 대안으로서, 배낭형태의 공개키 전송 시스템이 개발되었다. 이 방식은 초증가 수열의 성질을 공개

키에 숨기고 있다고 하여 이와 같은 명칭으로 불리게 되었다. 초증가 수열이라함은

$s_i > \sum_{j=1}^{i-1} s_j$ 을 만족하는 양의 정수로 구성된 일련의 정수의 집합

$s = (s_1, s_2, \ldots, s_n)$ 을 말한다. 이 방식은 RSA 전송시스템에 비해 암호화 및 복호화 속도가 빠른 것으로 알려져 있다. 이하에서는 배낭 형태의 공개 키 전송 시스템에 대하여 상세하게 기술하겠다.

배낭 형태의 공개 키 전송 시스템은 다른 공개 키 전송 시스템과 마찬가지로 개인키와 공개키를 생성하는 단계, 공개키에 의해 정보를 암호화하는 단계, 암호화된 신호를 전송하는 단계, 및 전송받은 암호화된 신호를 개인키에 의해 복호화하는 단계를 구비한다.

상기한 과정을 보다 세분하면, 먼저 개인키를 생성하고 그것으로부터 공개키를 생성한다. 이렇게 생성된 공개키를 사용하여 정보를 암호화한 후 이를 전송하면 수신자는 개인키를 사용하여 암호화된 정보를 복호화하게 된다. 이와 같은 과정을 예를 들어 설명면 다음과 같다.

먼저, 초증가 수열 B 를 (12, 17, 33, 74, 316) 와 같이 임의로 생성한다. 그 후, 초증가 수열 B 의 각 수를 모두 합산한 것보다 큰 수 M′ (예를 들면, 737로 정한다) 를 임의로 선택한다. 그 후, M′ 보다 작고, M′와 서로소인 수 W (예를 들어, 635 라 한다) 를 임의로 선택한다. 그 후, 초증가 수열 B 에 W 를 곱하고 M′ 에 의한 잉여류 연산을 한다. 그 결과를 공개키 A 라 하면,

$A = (W*B)(\mathrm{mod}\ M')$

$=\{635*(12, 17, 33, 74, 157, 316)\}\ (\mathrm{mod}\ 737)$

$= (250, 477, 319, 559, 200, 196)$ 와 같이 된다.

상기한 과정을 통해, 개인키 (B, M', W) 및 공개키 A 를 얻을 수 있으나 그 역의 과정 즉 공개키 A 로부터 개인키 (B, M', W) 를 생성하는 것은 용이하지 않다. 이와 같은 역연산의 용이성이 공개키 전송 시스템의 안전성을 가름하는 척도가 됨은 이미 설명한 바와 같다.

이제, 공개키 A 에 의해 정보 E (예를 들어 2진수 101101 라 한다)를 암호화하는 과정을 설명한다.

정보 E 를 공개키 A 에 곱함으로써 정보를 암호화한다. 즉, 암호화된 정보를 P 라 하면,

$P = A \cdot E$

$=(250, 477, 319, 559, 200, 196) \cdot (1, 0, 1, 1, 0, 1) = 1324$

와 같다. 이렇게 하여 암호화가 이루어 진다.

이와 같이 암호화된 신호를 전송하면 수신단에서는 전송받은 신호로부터 암화화되기 전의 정보를 추출한다 (복호화). 그 과정은 다음과 같다.

먼저, 암호화된 신호 P 에 W^{-1} (W^{-1} 는 $\{W*W^{-1}\}(\mathrm{mod}\ M')=1$ 이 되게 하는 양의 정수이다) 를 곱한 후 M' 에 의한 잉여류를 구한다. 그 값을 Q 라 하면

$Q = (W^{-1}*P)(\mathrm{mod}\ M')$

$= 435$ 가 된다.

여기서, P 를 $A \cdot E$ 로 치환하면,

$Q = (W^{-1}*A \cdot E)(\text{mod } M')$ 와 같고, 다시 A 를 $(W*B)(\text{mod } M')$ 으로 치환하면,

$\{W^{-1}*(W * B)(\text{mod } M') \cdot E\}(\text{mod } M')$ 와 같다.

W^{-1} 는 상수에 불과하므로 괄호 안으로 들어갈 수 있고, $W^{-1}*W$ 의 M'에 대한 잉여류는 1 이므로 결과식은,

$(B \cdot E)(\text{mod } M')$ 과 같다. E 를 $(e_1, e_2, e_3, e_4, e_5, e_6)$ 으로 정의 하고, 결과식을 수식으로 다시 표시하면,

$435 = \{(12, 17, 33, 74, 157, 316) \cdot (e_1, e_2, e_3, e_4, e_5, e_6)\}(\text{mod } 737)$ 와 같다.

여기서, (12, 17, 33, 74, 157, 316) 는 초증가 수열이므로 E 는 쉽게 구할 수 있다.

즉,

$435 = 12e_1 + 17e_2 + 33e_3 + 74e_4 + 157e_5 + 316e_6$ 로부터

암호화되기 전의 정보 E = (1, 0, 1, 1, 0, 1) 를 쉽게 추출할 수 있다.

그러나, 이 시스템은 Brickell, Lagarias 와 Odlyzko, Schnor 등이 개발한 공격법들에 의해 그 안전성에 심각한 타격을 입게 되었다. 즉, 수신자가 보유하고 있는 개인키를 제 3 자가 용이하게 찾아냄으로써, 정보데이터가 쉽게 유출되는 문제가 발생하였다. 그러한 대부분의 공격법은 격자기저 축소 알고리즘(Lattice Basis Reduction Algorithm)에 근거한 저밀도 (Low Density) 공격법에 의존하고 있다. 지금까지 배낭 문제 (Knapsack Problem) 형태의 공개키 전송시스템은 Chor-Rivest 에 의한 것을 포함, 매우 적은 수만이 그러한 공격법에 안전한 것으로 알려져 있다.

본 발명의 목적은 공개키를 용이하게 생성함으로써 전송 효율을 높이고, 공개키로부터 개인키를 추출하기가 보다 어렵게 함으로써 보다 높은 안전성을

확보하기 위해 개선된 배낭 형태의 공개키 전송 시스템을 제공하는 것이다.

【발명의 상세한 설명】

본 발명은 초증가 수열을 이용한 배낭 형태의 공개키 대신에 초증가 행렬렬을 이용한 배낭 형태 공개키 방식을 제공한다. 본 발명은 초증가 수열 대신 초증가 행렬렬을 사용함으로써 공개키 및 개인키들이 임의의 디멘젼을 갖는 행렬렬로 확장된다. 이것이 공개키로부터 개인키를 추출하기가 보다 어려워지는 이유가 된다. 따라서, 본 발명의 구성은 상술한 종래의 초증가 수열을 이용한 공개키 전송 시스템과 비교할 때, 초증가 수열대신 초증가 행렬렬을 생성한다는 것을 제외하고는 동일하다. 이와 같은 구성을 기술하면 다음과 같다.

본 발명은 k_1 및 k_2 가 양의 정수이며 $k_1 \times k_2$ 가 3 이상의 정수이고, n 이 2 이상의 정수라고 할 때,

$k_1 \times k_2$ 로 구성된 n 개의 행렬을 포함하는 개인키를 생성하는 단계;

개인키로부터 $k_1 \times k_2$ 로 구성된 n 개의 행렬을 포함하는 공개키를 생성하는 단계;

송신하고자 하는 이진정보를 n 개의 다수 개의 비트열 $E=\{e_1,e_2,...,e_n\}$, $e_i \in \{0,1\}$ 로 분할하는 단계;

다수개의 비트열 E 를 각각 공개키를 이용하여 암호화하는 단계;

암호화된 정보를 합체하여 전송 데이터 S 를 형성하는 단계;

전송 데이터 S 를 수신국에 전달하는 단계; 및

수신국은 수신된 상기 전송 데이터 S 를 개인키를 이용하여 이진정보

데이터를 추출하는 단계를 구비하고, 개인키를 생성하는 단계를 이진정보 데이터를 추출하는 단계 전에 구비하는 것을 특징으로 하는 이진 정보 보조 전송방법이다.

공개키를 생성한 후에, 공개키를 구성하는 각 행렬에 랜덤한 수를 더하거나/더하고, 순서 바꾸기 함수를 실행함으로써 공개키로부터 개인키를 추출하는 것을 보다 어렵게 할 수 있다. 상기의 경우에 있어서, 복호화하기 전에 일정한 수를 빼거나/빼고, 순서 바꾸기 함수의 역함수를 실행하여 전송하고자 하는 이진 정보 데이터 E 를 정확하게 추출할 수 있다.

이하에서는 도면을 참조하여 보다 상세하게 본 발명을 설명하겠다.

도 1은 이진 정보 데이터를 암호화하기 위한 개인키 및 공개키를 생성하는 과정을 나타낸 흐름도이다.

이 과정은 먼저 개인키 (cc_t, W_1, W_2, M) 를 생성하게 되는데, 여기서 cc_t 는 n개의 $K_1 \times K_2$ 초증가 행렬렬이며, W_1 은 $K_1 \times K_1$ 행렬이며, W_2 는 $K_2 \times K_2$ 행렬이며, 각각은 초증가 수열에 의한 배낭 형태의 공개키 전송 시스템에서의 B, W, M'에 대응하는 값이다.

먼저 양의 정수 k_1, k_2, l_1, l_2, ... ,l_u 를 $k_1 \times k_2 \geq 3,\ 2 \leq u \leq k_1 \times k_2 - 1$ 이 되도록 임의로 선택하고, $n = \sum_{s=1}^{u} l_s$ 라고 한다 (단계 110).

그 후, 각 s $(1 \leq s \leq u)$ 에 대하여 길이가 l_s 인 초증가 수열

(Superincreasing Integer Sequence) u 개를 선택하고 이것을

$d_s=(d_{s,1},d_{s,2},\ldots,d_{s,l_s})$, $1\le s\le u$ 라 한다 (120). 초증가 수열이

란 $d_{s,j}$ 가 양의 정수이면서 $\sum_{j=1}^{t} d_{s,j} < d_{s,t+1},\ (1\le t\le l_s-1)$ 인 수열을

말한다.

그 후, 행렬의 크기가 $k_1 \times k_2$ 이고 길이가 n 인 초증가 행렬열

(Superincreasing Matrix Sequence) 을 다음과 같이 생성한다 (단계 130). 이 행

렬열을 $cc_t=[cc_{t,(i,j)}]$ 라 하고, $1\le t\le n,\ 1\le i\le k_1,\ 1\le j\le k_2$ 이라 하면 각

$cc_{t,(i,j)}$ 는 다음과 같이 생성된다.

ⓐ (i,j)=(1,1) 인 경우 , $1\le t\le l_1$ 이면 $cc_{t,(1,1)} = d_{1,t}$ 로 하고,

$l_1+1\le t\le n$ 이면 $cc_{t,(1,1)}$ 는 $\sum_{t=l_1+1}^{n} cc_{t,(1,1)} < d_{1,1}$ 를 만족하는 임의의

양의 정수 (positive random integer) 로 선택한다.

ⓑ (i,j) 가 $2 \le (i-1)k_2 + j \le u-1$ 인 경우, $1\le t\le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ 이면

$cc_{t,(i,j)}$는 임의의 양의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_2+j-1} l_s+1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$ 이면

$cc_{t,(i,j)}=d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$ 로 하고, $\sum_{s=1}^{(i-1)k_2+j} l_s+1 \le t \le n$ 이면 $cc_{t,(i,j)}$는

$\sum_{t=\sum_{s=1}^{(i-1)k_2+j} l_s+1}^{n} cc_{t,(i,j)} < d_{(i-1)k_2+j,1}$ 를 만족하는 임의의 양의 정수로 선택한다.

ⓒ (i,j)가 (i−1)k2+j = u 인 경우는, $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ 이면 $cc_{t,(i,j)}$ 는 임의의 양의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_2+j-1} l_s+1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$ 이면

$cc_{t,(i,j)}=d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$ 로 한다.

ⓓ (i,j) 가 $u+1 \le (i-1)k_2+j \le k \times k_2-1$ 인 경우는, $cc_{t,(i,j)}$ 는 $1 \le t \le n$ 에서 임의의 양의 정수로 선택한다.

ⓔ (i,j) 가 $(i-1)k_2+j = k_1 \times k_2$ 인 경우는, $1 \le t \le n$ 에서 $cc_{t(i,j)}$

= 0 으로 선택한다.

그 후, 정수 M 을 다음과 같이 선택한다 (단계 140).

$$M > \mathrm{Max}\{d_{(s,1)} + \sum_{j=1}^{l_s} d_{s,j} \mid s = 1,2,\ldots,u\}$$

을 만족하는 임의의 양의 정수 M 을 선택한다.

그 후, n 개의 임의의 양의 정수 r_1 , r_2 , ... , r_n 을 선택한다(단계 150).

그 후, 행렬 cc_t 의 각 인수에 r_t 를 더한 후 M 에 의한 잉여류를 선택한 행렬 (수학식 1 에 나타낸 바와 같이 c_t 라 한다) 을 생성한다 (단계 160).

【수학식 1】

$$c_{t,(i,j)} \equiv cc_{t,(i,j)} + r_t \pmod{M}$$

그 후, { 1,2, ...,n } 에 대한 순서 바꾸기 함수 (permutation function) π 를 선택하여 $b_t = c_{\pi(t)}$ 를 생성한다 (단계 170). 상기 cc_t의 각 인수에 r_t 를 더하는 단계 (단계 150 및 160) 또는 순서 바꾸기 함수를 적용하는 단계 (단계 170) 는 공개키로부터 개인키를 추출하기가 보다 어렵도록 하기 위한 것으로서 경우에 따라 생략할 수도 있다.

그 후, 각각 크기가 $k_1 \times k_1$ 와 $k_2 \times k_2$ 이고, 행렬원소를 M 의 잉여

류에 의한 계산을 할 때 역행렬이 존재하도록 두 행렬 W_1 와 W_2 를 임의로 선택한다 (180). 이로써 개인키 cc_t (또는 b_1 , b_2 , ... , b_n), W_1 ,W_2 , M, π 이 완성된다.

다음은 위에서 구한 개인키로부터 공개키를 생성한다 (단계 190).

단계 (190)에서는 n 개의 행렬 $a_t, (1 \le t \le n)$ 를 다음과 같이 생성한다.

$a_t \equiv w_1 b_t w_2 \pmod{M}$ 으로 하며 a_t 의 각 원소는 0 과 M 사이에 오도록 한다. 이로서 공개키 $a_t = (a_1 , a_2 , \dots , a_n)$ 가 완성된다.

도 2는 도 1의 과정에서 구한 공개키를 이용하여 전송하고자 하는 정보를 암호화하는 과정을 나타낸 흐름도이다.

n개의 비트로 분할된 전송하고자 하는 정보와 공개키를 곱함으로써 암호화가 이루어진다 (단계 210 및 220).

E 가 0 과 1 만으로 된 길이가 n 인 암호화하고자 하는 정보이라고 하자.

즉, $E=(e_1,e_2,\dots,e_n),\ e_t \in \{0,1\}$ 이라 하자.

암호화는 전송하고자 하는 정보 E 와 공개키 a 를 곱함으로써 이루어지며, 암호화된 신호를 S라 하면, S 는 수학식 2 와 같이 표시 된다.

【수학식 2】

$$s=\sum_{t=1}^{n} e_t a_t.$$

도 3은 암호화된 신호에 대한 복호화과정을 나타낸 흐름도이다. 암호화된 신호 s 으로부터 E 를 추출하는 과정은 다음과 같다.

W_1 , W_2 의 M 에 대한 잉여류 연산 역행렬 w_1^{-1}, w_2^{-1} 을 구하고, 이들을 s에 곱함으로써 중간 단계 복호문을 생성한다 (단계 310 내지 330). 이렇게 생성된 결과를 S_1 이라 하면 S_1 은 수학식 3 과 같다.

【수학식 3】

$$s_1 \equiv w_1^{-1} s w_2^{-1} \pmod{M}$$

여기서 $s_1=[s_{1,(i,j)}]$ 은 $0 \le s_{1,(i,j)} < M$ 을 만족하는 행렬이며, 식 $s_1=\sum_{t=1}^{n} e_t b_t$ 이 성립한다. 식 $s_1=\sum_{t=1}^{n} e_t b_t$ 이 성립하는 이유는 $W_1W_1^{-1}$ 및 $W_2W_2^{-1}$ 이 각각 1이기 때문이다.

한편, $e'_t = e_{\pi^{-1}(t)}$ 이라 하면, $e_t = e'_{\pi(t)}$ 이고 $b_t = c_{\pi(t)}$ 이므로 다음식이 성립한다.

$$s_1 = \sum_{i=1}^{n} e_i b_i = \sum_{i=1}^{n} e'_{\pi(i)} c_{\pi(i)} = \sum_{i=1}^{n} e'_i c_i$$

그 후, 적절한 방정식의 구성과 수학적 귀납법을 이용하여 $(e'_1, e'_2, \ldots e'_n)$ 의 값을 아래와 같은 방법으로 구한다. 첫번째로 $(e'_1, e'_2, \ldots e'_{l_1})$ 의 값은 $s_{1,(1,1)} - s_{1,(k_1,k_2)} = \sum_{j=1}^{l_1} x_j d_{1,j}$ 의 방정식에서 $(x_1, x_2, \ldots x_{l_1})$ 의 해가 되는데 $(d_{1,1}, d_{1,2}, \ldots, d_{1,l_1})$ 이 초증가 수열이므로 x_j 의 값을 쉽게 구할 수 있다.

예를 들어, $s_{1,(1,1)} - s_{1,(k_1,k_2)}$ 를 계산한 값이 "130" 이고, 초증가 수열이 {30,74,147} 이라 하면, "130" 은 "147" 보다 작으므로 해는 "0" 으로 되고 연산을 행하지 않고, "130" 은 "74" 와 비교하는 단계가 수행된다. 이때 130-74 = 56 이므로 해는 "1" 로 처리된다. 마지막으로 "56" 은 "30" 과 비교할 때 "56" 이 "30" 보다 크므로 해는 "1" 로 셋팅된다. 따라서 구하고자 하는 최종 해는 {1,1,0} 가 된다. 이것은 이 분야의 통상의 지식인에게는 일반적으로 알려진 것이다.

그 후, 수학적 귀납법의 가정으로서 $(e'_1, e'_2, \ldots e'_w)$ 의 값을 구했다고

가정하자. 여기서 $w=l_1+l_2+\ldots+l_v$ 이고 $v\in\{1,2,\ldots,u-1\}$ 이다. 그러면, $(e'_{w+1},e'_{w+2},\ldots.e'_{w+l_{v+1}})$ 의 값은 다음과 같은 방법으로 구한다.

$s_v=s_1-\sum_{t=1}^{w}e'_t c_t$ 로 놓고

$s_{v,([w/k_2]+1,v+1-[w/k_2]\cdot k_1)}-s_{v,(k_1,k_2)}=\sum_{j=1}^{l_{v+1}}x_{w+j}\,d_{v+1,j}$ 의 방정식에서

$(x_{w+1},x_{w+2},\ldots,x_{w+l_{v+1}})$ 의 값을 구하면 되는데, 역시 $(d_{v+1,1},d_{v+1,2},\ldots,d_{v+1,l_{v+1}})$ 가 초증가인 성질을 이용하면 쉽게 $(e'_{w+1},e'_{w+2},\ldots,e'_{w+l_{v+1}})$ 를 구할 수 있다. 이 귀납적 방법으로 $(e'_1,e'_2,\ldots,e'_n)$ 을 모두 구한다.

그 후, $e_t=e'_{\pi(t)}$ 인 성질을 이용하여 원래 메시지

$E=(e_1,e_2,\ldots,e_n)$ 을 다음과 같이 구한다.

$$E=(e_1,e_2,\ldots,e_n)=(e'_{\pi(1)},e'_{\pi(2)},\ldots,e'_{\pi(n)})$$

상술한 과정을 통해 암호화되기 전의 신호 E를 복원하였다.

이 방식에 의한 공개키 전송 시스템은 다른 공개키 전송시스템에 비해 속도 면에서 월등하며 이를 표 1에 나타내었다.

【표 1】

	본 발명	NTRU	RSA
연산화 속도	n	n^2	n^2
역 연산화 속도	n	n^2	n^2
연산키 길이	n^2	n	n
역 연산키 길이	n^2	n	n
메시지 확장 정도	1.5 - 1	3 or 4 -1	1 - 1

표 1 에 도시한 바와 같이, 본 발명은 기존의 NTRU 또는 RSA 시스템에 비하여 암호화 및 복호화 속도가 상당히 빠름을 알 수 있다. 공개키 길이 및 개인키 길이가 길이가 길어지는 문제는 현재 사용중인 시스템의 메모리 성능의 향상으로 인하여 거의 문제가 되지 않는다.

【도면의 간단한 설명】

도 1은 본 발명에 따라 개인키 및 공개키를 생성하는 과정을 나타낸 흐름도이다.

도 2는 본 발명에 따라 공개키를 사용하여 암호화하는 과정을 나타낸

흐름도이다.

도 3은 본 발명에 따라 개인키를 사용하여 복호화하는 과정을 나타낸 흐름도이다.

【산업상이용가능성】

본 발명에 따른 이진 정보 보호 전송방법은 초증가 수열을 사용한 배낭 형태의 공개키 전송 시스템이 갖는 저밀도 (low density) 공격법에 대한 취약성을 극복하고, 주연산이 덧셈이거나 또는 두 수의 비교이므로 컴퓨터 상에서 실현하는 데 속도가 매우 빨라 RSA 전송 시스템이 갖는 속도에서의 취약점을 극복할 수 있다.

따라서, 본 발명은 이진 정보를 전송 매체를 통하여 전송할 경우, 제 3 자가 용이하게 판독할 수 없도록 함과 동시에 전송 속도를 높일 수 있으므로 홈뱅킹, 전자상거래, 인터넷상에서의 정보교환 등에 직접 응용될 수 있는 효과가 있다.

상기에서는 본 발명의 상기의 특별한 실시예를 참조하여 기술하였지만, 본 기술이 속하는 분야에서의 당업자에게는 여기에 첨부된 특허청구범위의 정신 및 범위를 벗어남이 없이 다양한 형태의 변형 및 수정이 가능하다는 것이 충분히 이해될 수 있을 것이다.

【청구의 범위】

【청구항 1】

전자 전송 매체를 통하여 다수 개의 비트로 구성된 이진정보를 송신국으로부터 수신국으로 안전하게 전송하는 방법에 있어서, k_1 및 k_2 가 양의 정수이고, $k_1 \times k_2$ 가 3 이상의 정수이고, n 이 2 이상의 정수일 때,

$k_1 \times k_2$ 로 구성된 n 개의 행렬을 포함하는 개인키를 생성하는 단계;

상기 개인키로부터 $k_1 \times k_2$ 로 구성된 n 개의 행렬을 포함하는 공개키 (행렬렬 a_t)를 생성하는 단계;

상기 이진정보를 n 개의 다수 개의 비트열 $E=\{e_1,e_2,...,e_n\}$, $e_i \in \{0,1\}$ 로 분할하는 단계;

상기 다수개의 비트열 E 를 각각 상기 공개키를 이용하여 암호화하는 단계;

상기 암호화된 정보를 합체하여 암호화된 전송 데이터 S 를 형성하는 단계;

상기 암호화된 전송 데이터 S 를 전송하는 단계; 및

수신된 상기 암호화된 전송 데이터 S 를 상기 개인키를 이용하여 상기 이진정보 데이터를 추출하는 단계를 포함하는 것을 특징으로하는 이진 데이터 보호 전송방법.

【청구항 2】

제 1 항에 있어서,

상기 개인키를 형성하는 단계는

2 이상이고 $k_1 \times k_2 - 1$ 이하인 임의의 정수 u 를 선택하고, u 개의 양의 정수

$l_1, l_2, \ldots, l_u$ 를 선택하고, $l_1+l_2+\ldots+l_u$ 의 총합으로 되는 정수 n 을 설정한 후,

$1 \leq s \leq u$ 의 관계를 만족하는 각 s 에 대하여 길이가 l_s 인 초증가 수열 $d_s=(d_{s,1}, d_{s,2}, \ldots, d_{s,l_s})$ 로 표시되는 u 개의 초증가 수열 $d_1, d_2, \ldots, d_u$ 를 형성하는 단계;

$Max\left\{ d_{(s,1)}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u \right\}$ 보다 큰 임의의 정수 M 을 선택하는 단계;

각 행렬 원소를 M 의 잉여류로 계산할 때, 역행렬이 존재하는 임의의 $k_1 \times k_1$ 로 구성된 행렬 w_1 및 $k_2 \times k_2$ 열로 구성된 행렬 w_2 를 형성하는 단계;

(i,j)=(1,1)인 경우에, $1 \leq t \leq l_1$ 이면 $cc_{t,(1,1)} = d_{1,t}$ 로 하고, $l_1+1 \leq t \leq n$ 이면 $cc_{t,(1,1)}$는 양의 임의의 정수로 선택하되 $\sum_{t=l_1+1}^{n} cc_{t,(1,1)} < d_{1,1}$ 를 만족하는 범위에서 선택하고,

(i,j)가 $2 \le (i-1)k_2+j \le u-1$ 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$ 이면 $cc_{t,(i,j)} = d_{(i-1)k_2+j,\, t-\sum_{s=1}^{(i-1)k_2+j-1} l_s}$ 로 하고, $\sum_{s=1}^{(i-1)k_2+j} l_s + 1 \le t \le n$ 이면 $cc_{t,(i,j)}$는 $\sum_{s=1}^{n} cc_{t,(i,j)} < d_{(i-1)k_2+j,1} - \sum_{s=1}^{(i-1)k_2+j} l_s + 1$ 를 만족하는 임의의 양의 정수로 선택하고,

(i,j)가 $(i-1)k_2+j = u$ 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ 이면 $cc_{t,(i,j)}$는 임의의 양의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$ 이면 $cc_{t,(i,j)} = d_{(i-1)k_2+j,\, t-\sum_{s=1}^{(i-1)k_2+j-1} l_s}$ 로 하고,

(i,j) 가 $u+1 \le (i-1)k_2+j \le k_1 \times k_2 - 1$ 인 경우에 $cc_{t,(i,j)}$, $1 \le t \le n$ 는 임의의 양의 정수로 선택하고,

(i,j) 가 $(i-1)k_2+j = k_1 \times k_2$ 인 경우는 $1 \le t \le n$ 에서 $cc_{t(i,j)} = 0$

으로 선택하여 $k_1 \times k_2$ 로 구성되는 n 개의 행렬 $cc_{t,(i,j)}$ 를 형성하는 단계;

및

행렬 cc_t 에 식 $c_{t,(i,j)} \equiv cc_{t,(i,j)} \pmod{M}$ 과 같이 M 의

잉여류를 계산하는 단계를 포함하며,

상기 공개키를 생성하는 단계는

식 $a_t = w_1 \, cc_{t,(i,j)} \, w_2 \pmod{M}$ 를 만족하는 a_t 를

생성함으로써 이루어지며,

상기 암호화된 전송 데이터 S 를 형성하는 단계는 식 $s = \sum_{t=1}^{n} e_t a_t$ 을

만족하는 S를 생성함으로써 이루어지며, 상기 M 을 선택하는 단계 및 상기 w_1 과 w_2 를 생성하는 단계는 상기 초증가 행렬렬 cc_t 을 형성하는 단계 후이고 공개키를 형성하는 단계 전에 이루어지는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【청구항 3】

제 2 항에 있어서,

n 개의 임의의 양의 정수 r_1, r_2,...,r_n 을 선택한 후, $cc_{t,(i,j)}$ 를 형성하는 단계 및 M 의 잉여류를 계산하는 단계 사이에 행렬 cc_t 의 각 인수에 r_t 를 더하는 단계를 더 구비하는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【청구항 4】

제 2 항 또는 제 3 항 중 어느 한 항에 있어서,

cc_t 의 각 인수에 r_t 를 더하는 단계 또는 r_t 를 더하는 단계가 없는 경우에는 $cc_{t,(i,j)}$ 를 형성하는 단계 및 M 의 잉여류를 계산하는 단계 사이에 n 개의 행렬로 구성된 $cc_{t,(i,j)}$ 행렬에 대한 순서 바꾸기 함수를 실행하는 단계를 더 구비하는 것을 특징으로 하는 이진 정보 데이터 전송방법.

【청구항 5】

제 2 항 또는 제 3 항 중 어느 한 항에 있어서,

상기 이진정보 데이터를 추출하는 단계는

w_1, w_2 의 M 에 대한 잉여류연산의 역행렬 w_1^{-1}, w_2^{-1} 를 생성하는 단계;

상기 역행렬을 이용하여 하기의 식에 따라 행렬 s_1 를 생성하는 단계;

$$s_1 = \sum_{t=1}^{n} e_t b_t = w_1^{-1} s w_2^{-1}$$ (여기서 e_i 는 "0" 과 "1" 의 함수이고, b_t 는 $k_1 \times k_2$ 의 행렬임)

$s_{1,(1,1)} - s_{1,(k_1,K_2)}$ 로부터 제 1 비교값을 계산하는 단계;

상기 제 1 비교값과 초증가수열 $\{d_{11}, d_{12}, \ldots, d_{1l_1}\}$ 로부터 $(e_1, e_2, \ldots, e_{l_1})$ 의 제 1 이진정보를 얻는 단계;

v 가 2 의 값을 갖고, $w = \sum_{j=1}^{v} l_j$ 이라 할 때,

$s_{v,([w/k_2]+1,\, v+1-[w/k_2]\cdot k_1)} - s_{v,(k_1,k_2)}$ 로부터 제 v 번째 비교값을 계산하는 단계;

상기 제 v 번째 비교값과 초증가 수열 $(d_{v+1,1}, d_{v+1,2}, \ldots, d_{v+1,l_{v+1}})$ 로부터 $(e_{w+1}, e_{w+2}, \ldots, e_{w+l_{v+1}})$ 의 제 v 번째 이진정보를 구하는 단계; 및

상기 제 v 번째 비교값을 계산하는 단계와 제 v 번째 이진정보를 구하는 단계는 v 가 3부터 u 값까지 반복하는 단계를 포함하는 것을 특징으로 하는 이진 정

보 데이터 보호 전송방법.

【청구항 6】

제 4 항에 있어서,

상기 이진정보 데이터를 추출하는 단계가

w_1, w_2 의 M 을 잉여류로 하여 역행렬 w_1^{-1}, w_2^{-1} 를 형성하는 단계;

상기 역행렬을 이용하여 하기의 식에 따라 행렬 s_1 를 형성하는 단계;

$$s_1 = \sum_{t=1}^{n} e_t b_t = w_1^{-1} s w_2^{-1}$$

(여기서 e_i 는 "0" 과 "1" 의 함수이고, b_t 는 $k_1 \times k_2$ 의 행렬임)

$s_{1,(1,1)} - s_{1,(k_1,K_2)}$ 로부터 제 1 비교값을 계산하는 단계;

상기 제 1 비교값과 초증가수열 $\{d_{11}, d_{12}, \cdots, d_{1l_1}\}$ 로부터 $(e_1, e_2, \cdots, e_{l_1})$ 의 제 1 이진정보를 얻는 단계;

v 가 2 의 값을 갖고, $w = \sum_{j=1}^{v} l_j$ 이라 할 때,

$s_{v,([v/k_2]+1,\, v+1-[v/k_2]\cdot k_2)} - s_{v,(k_1,k_2)}$ 로부터 제 v 번째 비교값

을 계산하는 단계;

상기 제 v 번째 비교값과 초증가 수열 $(d_{v+1,1}, d_{v+1,2}, \cdots, d_{v+1,l_{v+1}})$ 로부터

$(e_{w+1}, e_{w+2}, \cdots, e_{w+l_{v+1}})$ 의 제 v 번째 이진정보를 구하는 단계;

상기 제 v 번째 비교값을 계산하는 단계와 제 v 번째 이진정보를 구하는 단계는 v 가 3부터 u 값까지 반복하는 단계를 포함하는 단계; 및

상기에서 구한 $(e_1, e_2, \cdots, e_{l_u})$ 에 상기 순서 바꾸기 함수의 역함수를 적용하는 단계를 구비하는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【요약서】

【요약】

본 발명은 전자 전송매체를 통하여 이진정보를 전송하는 방법에 관한 것으로서, 이진 정보 데이터를 암호화하기 위한 준비단계로서 공개키 및 개인키를 생성하는 단계, 공개키를 이용하여 이진 정보를 암호화하는 단계, 및 복호화 단계를 포함하는 것으로서 암호화를 위한 공개키 및 개인키 생성에 있어서 초증가 행렬렬을 사용하는 것을 특징으로 한다.

【색인어】

공개키 전송시스템

METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a method for transmitting binary information through electronic transmission media, and more particularly to a method for encrypting and deciphering binary information in transmission with the use of super-increasing matrix sequence.

Description of the Related Art

In case of transmitting information through electronic transmission media in recent, especially in data transmission between computers, security matter is being gradually amplified. Actually, data transmitted through transmission lines is relatively easily overheard, which means that important information can pass to third party's hands. In order to prevent such risk, it is necessary to encrypt information for transmission not to be easily read by a third party.

For the encryption of information, various types of encryption methods have been proposed. The encryption methods are largely classified into a symmetric-key method and a public key method. The symmetric key method is a method of using a deciphering key identical to an encrypting key, and the public key method is a method of using a deciphering key different from an encrypting key. The symmetric key method has benefits in

in order to lower or control an information transmission rate of a transmitter. In case of requiring the buffers, some actions should be taken in order for information not to be lost when a signal indicating that a receiving station is not ready for receiving the information is generated.

In the meantime, as an alternative for overcoming the problem of the RSA transmission system, a public key transmission system of a knapsack type has been developed. The system is called "knapsack" since it hides the properties of a super-increasing integer sequence in the public key. The super-increasing integer sequence refers to a set of integers $S=(S_1, S_2, \ldots, S_n)$ composed of positive integers satisfying $S_i > \sum_{j=1}^{i-1}$. The system is known to have faster encryption and decryption speeds than the RSA transmission system. Hereinafter, the public key transmission system of the knapsack type will be described in detail.

The public key transmission system of the knapsack type includes steps of: producing a private key and a public key as in the other public key transmission systems, encrypting information with the public key; transmitting the encrypted signal; and deciphering the transmitted encrypted signal with the private key.

With the steps ramified, the private key is first produced and then the public key is produced from the produced private key. Information is encrypted by using the produced public key and then transmitted. A receiver uses the private key to decipher the encrypted information. Such step is described as below with an example.

If transmitting such encrypted signal, the information prior to the encryption is extracted from the transmitted signal in a receiving stage(deciphering). The step is as follows. That is, the encrypted signal P is multiplied by W^{-1}, wherein the W^{-1} is a positive integer of satisfying $\{W*W^{-1}\}(\text{mod } M')=1$, and then a residue class is obtained based on the M'. If the obtained value is Q, the Q is expressed as follows:

$$Q=(W^{-1}*P)(\text{mod } M')$$
$$=435$$

where, if the P is substituted with A • E, $Q=(W^{-1}*A \bullet E)$, and then if the A is substituted with $(W*B)(\text{mod } M')$, $Q=\{W^{-1}*(W*B)(\text{mod } M') \bullet E\}(\text{mod } M')$.

The W^{-1} is just a constant, so that the W^{-1} can be put in the parentheses. A residue class regarding the M' of the $W^{-1}*W$ is a 1, so that the result expression is $(B \bullet E)(\text{mod } M')$. If the E is defined as $(e_1, e_2, e_3, e_4, e_5, e_6)$, the result expression is re-expressed as follows:

$435=\{(12, 17, 33, 74, 157, 316) \bullet (e_1, e_2, e_3, e_4, e_5, e_6)\}(\text{mod } 737)$. Here, (12, 17, 33, 74, 157, 316) is the super-increasing integer sequence, so that the E can be easily obtained. That is, the information E=(1, 0, 1, 1, 0, 1) prior to the encryption can be easily extracted from $435 = 12e_1 + 17e_2 + 33e_3 + 74e_4 + 157e_5 + 316e_6$.

However, the system is severely affected in its safety by attack methods developed by Brickell, Lagarias, and Odlyzko, Schnor, et al. That is, a private key of a receiver is easily found by a third party, so that a problem information data is easily leaked has occurred. Most of such attach methods rely upon a low density attack method based on the Lattice Basis

of: producing a private key including n matrices composed of $k_1 \times k_2$; producing a public key including n matrices composed of $k_1 \times k_2$ from the private key; dividing binary information to be transmitted into n plural bit sequences $E = \{e_1, e_2, \ldots, e_n\}$, $e_i \in \{0, 1\}$; encrypting the plural bit sequences E by using respective public keys; forming transmission data S by incorporating encrypted information; transmitting the transmission data S to a receiving station; and extracting binary information data from the received transmission data S in the receiving station by using the private key, wherein the step for producing the private key is placed prior to the step for extracting the binary information data.

After producing the public keys, an addition of a random number to respective matrices composing of the public keys and/or the execution of an order change function can make the extraction of a private key from the public key difficult. In the above case, binary information data E to be transmitted can be exactly extracted by adding a certain number and/or executing an inverse function of the order change function before deciphering.

BRIEF DESCRIPTION OF THE DRAWINGS

The above object and other advantages of the present invention will become more apparent by describing the preferred embodiment thereof in more detail with reference to the accompanying drawings, in which:

FIG. 1 is a flow chart for showing a process of producing a private key and a public key according to an embodiment of the

After that, a super-increasing matrix sequence having a matrix size of $k_1 \times k_2$ and length n is produced as follows(step 130). If the matrix sequence is referred to as $cc_t = [cc_{t,(i,j)}]$ in $1 \le t \le n$, $1 \le I \le k_1$, $1 \le j \le k_2$, respective $cc_{t,(i,j)}$ are produced as follows.

ⓐ in case of (i,j)=(1,1), $cc_{t(1,1)} = d_{1,t}$ in $1 \le t \le l_1$ and $cc_{t(1,1)}$ has a random positive integer satisfying

$$\sum_{t=l_1+1}^{n} CC_{t,(1,1)} < d_{1,1}$$

in $l_1+1 \le t \le n$.

ⓑ in case that (i,j) satisfies $2 \le (i-1)k_2+j \le u-1$, $cc_{t,(i,j)}$ has a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$,

$$CC_{t(i,j)} = d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$$

in $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$,

and another random positive integer satisfying

$$t = \sum_{s=1}^{(i-1)k_2+j} l_s + 1 \quad CC_{t,(i,j)} < d_{(i-1)k_2+j,1}$$

in $\sum_{s=1}^{(i-1)k_2+j} l_s + 1 \le t \le n$.

ⓒ in case that (i,j) satisfies $(i-1)k_2+j = u$, $cc_{t(i,j)}$ has a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ and

$$CC_{t,(i,j)} = d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$$

in $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$.

ⓓ in case that (i,j) satisfies $u+1 \le (i-1)k_2+j \le k \times k_2-1$,

as follows.

Respective elements exist between 0 and M with $a_t \equiv w_1 b_t w_2 \pmod{M}$. Accordingly, the public key $a_t = (a_1, a_2, \ldots, a_n)$ are completed.

FIG. 2 is a flow chart for showing an encryption process of information to be transmitted by using the public key of FIG. 1.

The encryption is performed by multiplying the information to be transmitted, which is divided into n bits, by the public key(steps 210 and 220).

Let E be the information containing only 0 and 1 and having a length n.

That is, $E = (e_1, e_2, \ldots, e_n)$, $et \in \{0, 1\}$

The encryption is carried out by multiplying information E to be transmitted by a public key a. If an encrypted signal is indicated as S, the S may be expressed as Formula 2 as below:

Formula 2

$$S = \sum_{t=1}^{n} e_t a_t$$

FIG. 3 is a flow chart for showing a deciphering process with respect to an encrypted signal. A process for extracting E from the encrypted signal s is as follows.

W_1^{-1} and W_2^{-1} of residue class operation inverse matrices with respect to M of W_1 and W_2 are calculated and multiplied by s to produce a cyphertext of an intermediate step(steps 310 to 330). Let such result be S_1, then formula 3 is as follows.

Formula 3

$$s_1 \equiv w_1^{-1} s w_2^{-1} \pmod{M}$$

where, s_1 is a matrix satisfying $0 \leq s_{1,(i,j)} < M$, a formula

in $v \in \{1, 2, \ldots, u-1\}$, a value of $(e'_{w+1}, e'_{w+2}, \ldots, e'_{w+1v+1})$ is obtained as follows. That is, the value is obtained from the calculation of the value of $(x_{w+1}, x_{w+2}, \ldots, x_{w+1v+1})$ in an equation of $S_{v,([v/k_2]+1,v+1-[v/k_2]\cdot k_1)} - S_{v,(k_1,k_2)} = \sum_{j=1}^{l_{w+1}} x_{w+j} d_{v+1,j}$ when $S_v = S_1 - \sum_{t=1}^{w} e'_t c_t$. The use of a super-increasing property of $(d_{v+1,1}, d_{v+1,2}, \ldots, d_{v+1,1v+1})$ enables a value of $(e'_{w+1}, e'_{w+2}, \ldots, e'_{w+1v+1})$ to be easily obtained. All the values of $(e'_1, e'_2, \ldots, e'_n)$ are obtained through the mathematical induction method.

After that, the original message of $E = (e_1, e_2, \ldots, e_n)$ is obtained as follows through the use of the property of $e_t = e'_{\pi(t)}$. That is, $E = (e_1, e_2, \ldots, e_n) = (e'_{\pi(1)}, e'_{\pi(2)}, \ldots, e'_{\pi(n)})$
The signal E prior to the encryption is deciphered through the above process.

The public key transmission system based on this method is much better in a speed point of view, compared to the other public key transmission system and shown in Table 1.

Table 1

	Present invention	NTRU	RSA
Operation speed	n	n^2	n^2
Inverse operation speed	n	n^2	n^2
Operation key length	n^2	n	N
Inverse operation key length	n^2	n	N
Message extension degree	1.5-1	3 or 4-1	1-1

As shown in Table 1, the present invention has a much faster speed in the encryption and decryption, compared to the existing NTRU or RSA system. The matter of prolonging a public key length and a private key length does not cause any problem due to the improvement of the performance of system memories

CLAIMS

1. In a method for safely transmitting binary information constructed with plural bits through electronic transmission media, the method comprising steps of:

producing a private key including n matrices constructed with $k_1 \times k_2$, when k_1 and k_2 are positive integers, $k_1 \times k_2$ is an integer larger than 3, and n is an integer larger than 2;

producing a public key(matrix sequence a_t) including the n matrices constituted with the $k_1 \times k_2$ from the private key;

dividing the binary information into n plural bit sequences $E = \{e_1, e_2, \ldots, e_n\}$ in $e_i \in \{0, 1\}$;

encrypting the plural bit sequences E respectively by using the public key;

incorporating the encrypted information and forming encrypted transmission data S;

transmitting the encrypted transmission data S; and

extracting the binary information data from the encrypted transmission data S by using the private key.

2. The method as claimed in claim 1, wherein the step for producing the private key includes steps of:

forming u super-increasing integer sequences $d_1, d_2, \ldots, d_u$ expressed as $d_s = (d_{s,1}, d_{s,2}, \ldots, d_{s,ls})$ of a super-increasing integer sequence having a length l_s with respect to each S satisfying a relationship of $1 \leq s \leq u$, after arbitrarily selecting an integer n larger than 2 but less than $k_1 \times k_2 - 1$, selecting u positive integers $l_1, l_2, \ldots, l_u$, and setting the integer n of a total sum of $l_1 + l_2 + \ldots + l_u$;

selecting a random integer M larger than

a) a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$, and

b) $cc_{t,(i,j)} = d_{(i-1)k_{2+j,t-}}$ in $\sum_{s=1}^{(i-1)k_2+j-1} l_s$

$$\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s,$$

4) if (i,j) satisfies $u + 1 \le (i-1)k_2 + j \le k_1 \times k_2 - 1$, a random positive integer in $1 \le t \le n$, and

5) if (i,j) satisfies $(i-1)k_2 + j = k_1 \times k_2$, "0"; and

calculating a residue class of M as in $c_{t,(i,j)} \equiv cc_{t,(i,j)} \pmod{M}$, wherein the step for producing the public key is accomplished by producing at satisfying $a_t = w_1\ cc_{t,(i,j)}\ w_2 \pmod{M}$, the step for forming the encrypted transmission data S is accomplished by producing the S satisfying a formula $S_1 = \sum_{t=1}^{n} e_t a_t$, and the steps for selecting the M and producing the w_1 and w_2 is carried out after the step for forming the super-increasing matrix sequence cc_t and before the step for forming the public key.

3. The method as claimed in claim 2, further comprising a step, after selecting n random positive integers r_1, r_2, ..., r_n, for adding r_t to respective elements between the step for forming the $cc_{t,(i,j)}$ and the step for calculating the residue class of M.

4. The method claimed in claim 2 or 3, further comprising a step, in case that there does not exist the step for adding r_t

forming a matrix s_1 according to a following formula by using the inverse matrices:

$$S_1 = \sum_{t=1}^{n} e_t a_t = w_1^{-1} s w_2^{-1}$$

, wherein e_i is a function of "0" and "1" and b_t is a matrix of $k_1 \times k_2$;

calculating a first comparison value from $s_{1,(1,1)} - s_{1,(k1,k2)}$;

obtaining first binary information of (e_1, e_2, ..., e_{l1}) from the first comparison value and a super-increasing integer sequence {d_{11}, d_{12}, ..., d_{1l1}};

calculating a vth comparison value from $s_{v,([v/k2]+1,\ v+1-[v/k2] \cdot k2)} - s_{v,(k1,k2)}$ when the v has a value of 2 and $w = \sum_{j=1}^{v} l_j$;

obtaining vth binary information of (e_{w+1}, e_{w+2}, ..., e_{w+lv+1}) from the vth comparison value and a super-increasing integer sequence ($d_{v+1,1}$, $d_{v+1,2}$, ..., $d_{v+1,lv+1}$);

iterating the step for calculating the vth comparison value and the step for obtaining the vth binary information till the v has values from 3 to u; and

applying an inverse function of the permutation function) to the (e_1, e_2, ..., e_{lu}).

FIG.1

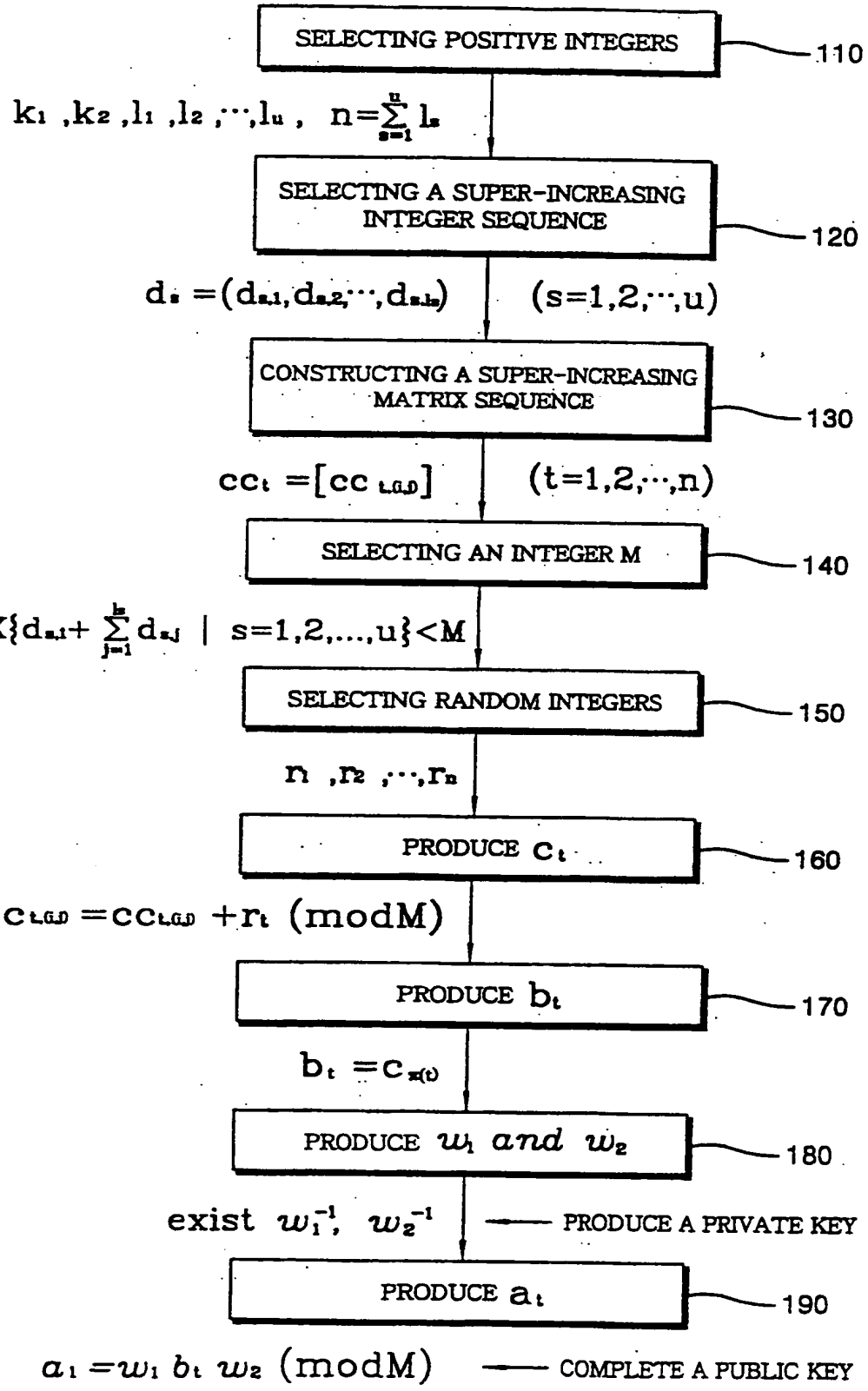

SELECTING POSITIVE INTEGERS
110
$k_1, k_2, l_1, l_2, \cdots, l_u, \quad n=\sum_{s=1}^{u} l_s$
SELECTING A SUPER-INCREASING INTEGER SEQUENCE
120
$d_s=(d_{s,1}, d_{s,2}, \cdots, d_{s,l_s}) \quad (s=1,2,\cdots,u)$
CONSTRUCTING A SUPER-INCREASING MATRIX SEQUENCE
130
$cc_t=[cc_{t,0}] \quad (t=1,2,\cdots,n)$
SELECTING AN INTEGER M
140
$MAX\{d_{s,1}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u\}<M$
SELECTING RANDOM INTEGERS
150
$r_1, r_2, \cdots, r_n$
PRODUCE c_t
160
$c_{t,0}=cc_{t,0}+r_t \pmod{M}$
PRODUCE b_t
170
$b_t=c_{\pi(t)}$
PRODUCE w_1 and w_2
180
exist w_1^{-1}, w_2^{-1}
PRODUCE A PRIVATE KEY
PRODUCE a_t
190
$a_t=w_1 b_t w_2 \pmod{M}$
COMPLETE A PUBLIC KEY

FIG.2

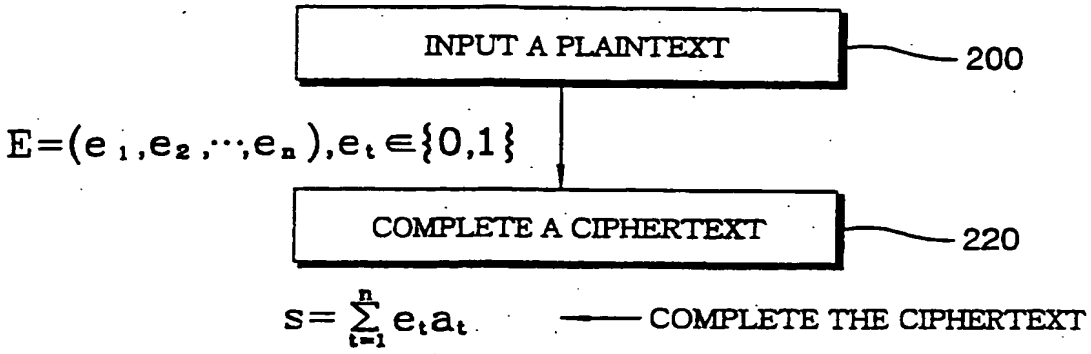
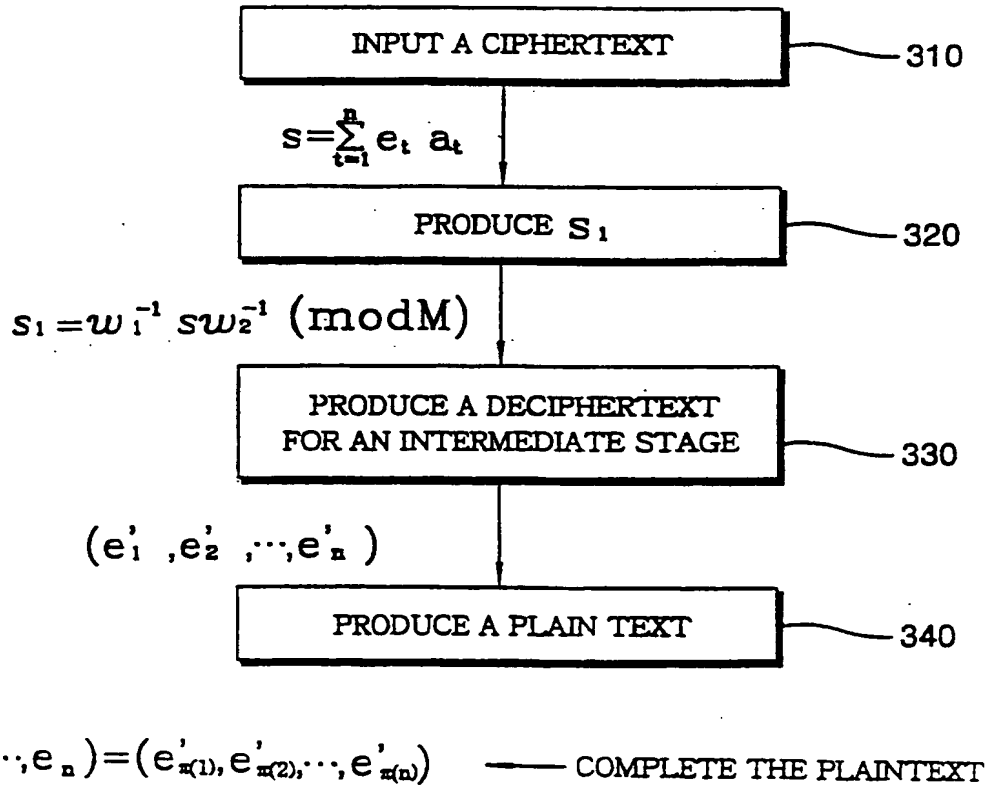


FIG.3



$E=(e_1,e_2,\cdots,e_n)=(e'_{\pi(1)}, e'_{\pi(2)}, \cdots, e'_{\pi(n)})$ —— COMPLETE THE PLAINTEXT

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR00/00640

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04B 1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)
IPC7 H04M 1/00

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search trerms used)
Patrom
FPD, PAJ, WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5872846 A (MCI Communicatios Corporation) 16 FEB. 1999 See the entire document	1
A	KR 98-77685 A (LG Electronic CORP.) 16 NOV. 1998 See the entire document	1
A	KR 98-35958 A (LG Electronic CORP.) 5 AUG. 1998 See the abstract and background of the invention	1
A	US 5592554 A (Siemens Aktiengesellschaft) 7 JAN. 1997 See the abstract and column 2	1
A	US 5588061 A (Bell Atlantic Network Services Inc., Bell communications Research Inc.) 24 DEC. 1996 See the abstract and claims	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 OCTOBER 2000 (18.10.2000)	18 OCTOBER 2000 (18.10.2000)

Name and mailing address of the ISA/KR
Korean Industrial Property Office
Government Complex-Taejon, Dunsan-dong, So-ku, Taejon
Metropolitan City 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
JEONG, Hyun Su
Telephone No. 82-42-481-5949

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR00/00640

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04B 1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)

IPC7 H04M 1/00

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search trerms used)

Patrom
FPD, PAJ, WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5872846 A (MCI Communicatios Corporation) 16 FEB. 1999 See the entire document	1
A	KR 98-77685 A (LG Electronic CORP.) 16 NOV. 1998 See the entire document	1
A	KR 98-35958 A (LG Electronic CORP.) 5 AUG. 1998 See the abstract and background of the invention	1
A	US 5592554 A (Siemens Aktiengesellschaft) 7 JAN. 1997 See the abstract and column 2	1
A	US 5588061 A (Bell Atlantic Network Services Inc., Bell communications Research Inc.) 24 DEC. 1996 See the abstract and claims	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 OCTOBER 2000 (18.10.2000)	18 OCTOBER 2000 (18.10.2000)

Name and mailing address of the ISA/KR	Authorized officer
Korean Industrial Property Office Government Complex-Taejon, Dunsan-dong, So-ku, Taejon Metropolitan City 302-701, Republic of Korea	JEONG, Hyun Su
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5949

Form PCT/ISA/210 (second sheet) (July 1998)